A policy and program for invigorating science and technology for national security

Consultation Paper – April 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A policy and program for invigorating science and technology for national security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence Science and Technology Organisation,Department of Defence, , ,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

A national security science and technology policy and program

Consultation Paper – April 2014

The Government is seeking the views of stakeholders from all sectors of Australia's national security science and technology (S&T) community – including national security government agencies (federal and state), universities, publicly funded research agencies, other research agencies and industry, to help develop a new policy and program management framework for achieving a whole-of-government approach to national security science and technology. The policy will articulate the strategic direction for national security S&T over the next decade, and will provide the mechanisms to deliver a coordinated National Security S&T Program. The Program will involve multiagency, multidisciplinary collaborations, of short to long-term focus, aimed at delivering tangible operational and capability outcomes for national security user agencies.

National security S&T community stakeholders from government, academia and industry are invited to make submissions on the policy and program management framework, including proposed priority areas for national security S&T. A series of questions throughout this paper provide prompts that may help structure your response. The government will consider all feedback received before finalising the national security S&T policy and program management framework.

Submissions can be lodged in the following ways:

Email: NSSTC@dsto.defence.gov.au

Post: Director, Science Strategy and Policy Branch

Defence Science and Technology Organisation

Department of Defence

PO Box 7931

Canberra ACT 2610

Submissions should be received by **5.00pm, 1 May 2014**.

Table of Contents

1. Introduction

The Hon Stuart Robert MP, Assistant Minister for Defence is championing the development of a new framework for achieving a whole-of-government approach to national security S&T. The framework will comprise a national security S&T policy statement and supporting Program. The intention is to transition from poorly coordinated and under-resourced S&T effort to a collaborative co-investment approach between government, academia and industry that effectively and efficiently delivers innovative S&T solutions in priority national security areas for Australia.

The Defence Science and Technology Organisation (DSTO) is responsible for leading and coordinating national security S&T, a role transferred from the Department of the Prime Minister and Cabinet to the Department of Defence in February 2012. As part of that role, DSTO is leading the development of a new policy and supporting program in consultation with the national security S&T communities, for consideration and endorsement by Government in 2014.

The national security S&T policy will:

- enunciate the Government's priorities for national security S&T,
- provide a means by which S&T investment can be balanced to support short-term national security operational needs in addition to enduring security challenges,
- establish an efficient management and governance framework that delivers S&T outcomes to national security agencies, and
- encourage shared public and private investment in national security S&T, and facilitate commercialisation of research outcomes for national benefit.

The policy will be delivered through a coherent and coordinated national security S&T program that address national security S&T priorities and delivers real tangible outcomes for national security users.

The national security S&T policy and supporting program will harness S&T providers, including publicly funded research agencies (PFRAs), universities and industry to benefit national security 'user' agencies, including policy agencies, regulators, emergency response agencies, policing and law enforcement agencies, border protection agencies and the intelligence community.

This paper aims to promote discussion and elicit input from government agencies and the S&T community that will assist in developing a national security S&T policy and program that will improve the delivery and application of S&T to address Australia's national security challenges now and into the future.

2. Background

2.1 S&T is important to Australia's national security

In an uncertain and high risk security environment, Australia's scientific and technological base is one of our greatest national security assets. S&T underpins Australia's capability to prevent, prepare for, respond to and recover from security threats. Australia's S&T positions us to meet current threats and allows us to adapt and exploit emerging technologies to counter potential future threats. S&T can and is contributing to improving our national security capabilities in intelligence and surveillance, prevention, protection, interdiction, response and recovery.

Technology and innovation saves money through efficiency (doing the same things, but in smarter ways), making available and making better use of cheaper more efficient tools and technologies, changing operating models (doing smarter things to get desired outcomes) and through smart buyer advice, ensuring the national security agencies are well informed about technology options. Predictive tools help us move from reactive response to proactive planning and to better utilise scarce resources (e.g. border surveillance and monitoring). Simpler earlier interventions can address issues before they become major security threats or there are risks of significant operational failure or major increases in operating costs.

S&T also plays a critical support role in strategic planning, policy development, capability analysis, operational planning and assessment, standards development, systems interoperability and integration, and risk-informed strategic decision-making.

More broadly than national security, creating technological innovations and building world class S&T capabilities and national S&T infrastructure, can boost our productivity, our industries and our skills, resulting in long term benefits for our economy and higher living and education standards[1,2].

Questions for discussion:

Q2.1 Are there other imperatives or drivers that justify the creation of a national security S&T policy and program?

2.2 The national security S&T community

The following table taken from the Guide to Australia's National Security Capabilities (2013) [3] identifies agencies that maintain capabilities in support of Australia's national security functions. These agencies, together with state and territory counterparts, comprise the national security user community. S&T supports the development and enhancement of all these capabilities.

[1] Professor Ian Chubb, Australia's Chief Scientist, The nation's scorecard on science and future scenarios to 2025, Speech delivered to Australia-Israel Chamber of Commerce, 29 February 2012.
[2] Office of the Chief Scientist (2012). Health of Australian Science.
[3] Attorney-General's Department (2013), Guide to Australia's National Security Capability, 2013

NATIONAL SECURITY FUNCTIONS	NATIONAL SECURITY AGENCIES WITH CAPABILITIES WHICH ALIGN TO FUNCTIONS*
Threat detection, recognition, identification and monitoring	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Intelligence, information and knowledge sharing and dissemination	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Horizon scanning, risk assessment, modelling and simulation	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
National oversight, command, control and coordination	ACBPS, ACC, AFP, AGD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Public engagement, media and warnings	ACBPS, ACC, AFP, AGD, DAFF, Defence DFAT, DIT, DOHA, PM&C
Incident response, law enforcement, investigation and forensics	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C
Quarantine, containment, render safe, decontamination and disposal	ACBPS, AFP, DAFF, Defence, DFAT, DIT, DOHA
Community and infrastructure resilience and recovery	ACBPS, AFP, AGD, AGO, DAFF, Defence, DFAT, DIAC, DIT, DOHA
Policy, national governance and capability development	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
International engagement	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Testing, exercise and evaluation	ACBPS, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIT, PM&C, ONA
Mass care, mass casualty and mass fatality management	AFP, Defence, DFAT, DIAC, DIT, DOHA
Stockpiles, logistics and distribution	AFP, AGD, AusAID, Defence, DFAT, DIT, DOHA

**Refer to the Glossary for an explanation of acronyms.*

Australia undertakes world-leading national security S&T through PFRAs, universities and industry. Some national security agencies such as the Australian Federal Police have established science and technology capabilities. The following are key PFRAs undertaking S&T vital to our national security:

- The Australian Institute of Criminology (AIC)
- The Australian Nuclear Science and Technology Organisation (ANSTO)
- The Commonwealth Scientific and Industrial Research Organisation (CSIRO)
- The Defence Science and Technology Organisation (DSTO)
- Geoscience Australia
- National Information and Communications Technologies Australia (NICTA)
- The National Measurement Institute (NMI)

Some universities have established centres dedicated to national security related research (e.g. Australian National University, Edith Cowan University, Macquarie University) and the majority of universities run programs relevant to national security. Industry undertakes approximately sixty percent

of Australia's research and development, predominantly focused on applied research. The private sector plays two further essential roles in national security S&T. First, as owners and operators of critical infrastructure (including utilities, transport and communications), private sector organisations can drive the uptake of new technology and knowledge. Second, private sector organisations are essential to the commercialisation of research[4].

It is essential that user agencies clearly articulate their national security needs or capability requirements and that S&T providers understand and translate those requirements into S&T projects that will deliver the maximum benefit in relation to costs. DSTO's role, as the national coordinator for national security S&T is to facilitate the effective translation of needs into outcomes and to ensure the community as a whole makes wise S&T investment decisions, guided by the right policy framework.

2.3 Challenges and opportunities

As part of the policy development process, DSTO conducted a survey in 2013 to better understand the nature and extent of challenges being faced by national security user agencies and S&T providers in providing and sourcing S&T support. To complement the survey, a workshop was held in November 2013, bringing key national security S&T stakeholders together to identify key issues which the Government's policy framework might address.

The table below summarises the key issues raised through the survey and workshop by the user agencies, policy agencies and S&T providers. The issues centre around four themes – user requirements or priorities, S&T support, resourcing and delivery.

Table 1: Issues identified through the workshop and questionnaire (2013)

Issues	Stakeholders
User Requirements / Priorities	
Need greater clarity in national security priorities (scope) e.g. traditional, all hazard, national interest; and implications for user agency priorities	User agency
Lack of knowledge of shared problems across organisations and therefore lack of ability to collaborate and/or jointly fund research and development	
Lack of identified S&T opportunities	
Organizations face increasing challenges of keeping up with emerging technologies and minimising new security threats such as in advanced analytics, network analysis and data integration, 3D printing, cyber and electronic security, intelligence including data mining and data management, and border security including identity security	
Limited situational awareness of whole-of-government NS requirements for S&T support	Provider agency
Access to information (declassified where necessary) on NS requirements / priorities	
Challenges around access to independent S&T advice and support for capability development	Policy agency

[4] Department of the Prime Minister and Cabinet (2009), The National Security Science and Innovation Strategy

Issues	Stakeholders
S&T support	
Limited clarity on the S&T programs to meet NS requirements of user agencies.	User agency
Limited domestic S&T development to support new regulatory activities such as air cargo	
Lack of awareness of NS S&T capabilities	
Challenges around access to relevant research data such as developmental or experimental data sets for big data	Provider industry
Resources - $, FTE, Physical, IT	
High quality technical advice and input to policy in key areas such as Chemical and Biological weapons is limited to a single specialist	User agency
Shortage of skilled IT and security professionals	
In-house small analytical staff is stretched and difficulty in tapping scientific specialists to complement in-house staff and can effectively communicate with ministerial audiences	
Limitations in access or owning computational resources and associated skills to undertake mathematical modelling. Yet organisations called upon to nationally coordinate such activity in response to NS incidents	
S&T providers competing (not collaborating) for technical support – academia competes against industry often appearing as cheap labour but then without generating commercially viable or sustainable technological outputs	Provider industry
Suitable education (skilling) options in emerging areas such as big data is challenging	
Poor funding and resourcing. What is to be delivered is known.	Provider industry; User agency
Delivery	
No formalised mechanism to engage with DSTO and other S&T providers – publicly funded, academia or industry	Provider industry
Few mechanisms outside of pure research to engage with S&T providers	
Process to have new technology approved too bureaucratic keeping SME's out of the market	
DSTO provide greater transparency of S&T goals to enable industry to propose in which they can be supported.	
Few models exist that meet the security requirements of various users such as intelligence agencies.	Provider industry; User Agency

In summary, based on this feedback from stakeholders, key issues that this policy must address is the overall lack of transparency, visibility and accessibility of S&T efforts and expertise to collectively meet the needs of national security agencies.

Questions for discussion:

Q2.2 Are there any other challenges or opportunities that need to be addressed?

3. The policy context

3.1 Why a national security S&T policy?

Australia's approach to national security S&T has evolved and matured over the last decade in response to its changing strategic circumstances and government policy. Countering national security threats requires a national effort involving a range of government (Federal/state/territory), national bodies, the Australian Defence Force, industry -underpinned by science and research and the collective efforts of the S&T community. In 2009, the Government brought these stakeholders together and developed the National Security Science and Innovation Strategy (NSSIS) [5]. It was a strategy, based on key elements that have applicability today (see table below). However, implementation of NSSIS was not funded and many of its recommendations were not progressed. The intention in the current process is to use those parts of NSSIS that have utility and currency as the starting point for developing and implementing the new national security S&T policy and program.

Table 2: Policy elements of the National Security Science and Innovation Strategy 2009[6]

Recognises the importance of science and innovation in protecting our national security
Integrates science and innovation into broader national security policy coordination efforts
Incorporates the breadth and importance of national security requirements in science and innovation policy and funding programs
Develops specific mechanisms to bring together Australian Government national security science and innovation agencies

First and foremost, the national security S&T policy must align with and support the Government's national security and science and research agendas and priorities. Current areas of focus for the Government in national security include stronger Defence; improving foreign affairs – a stronger focus on the region; strengthening our alliance with the US; countering terrorism and tackling serious and organised crime. Cyber is also seen as a priority, given its pervasive and growing threat[7,8] and border integrity in relation to maritime arrivals[9]. The national security S&T policy will consider any shifts in priority or scope with the changes of government since NSSIS was developed and recognise DSTO's whole-of-government role in leading and coordinating national security S&T. The policy must also complement other major national security policy setting documents, such as the Defence White Paper,

[5] www.dsto.defence.gov.au/national security
[6] www.dsto.defence.gov.au/national security
[7] Minister for Foreign Affairs The Hon Julie Bishop MP, Address to the Seoul Cyberspace Conference 'Strengthening cross-border cooperation – an Australian Perspective. 17 October 2013.
[8] Minister for Communications The Hon Malcolm Turnbull MP, Launch of Strategy and Statecraft in Cyberspace research program. 5 March 2014
[9] Liberal Party of Australia (2013). '*Our Plan. Real Solutions for all Australians*.' http://www.liberal.org.au/our-plan

the Defence Capability Plan and Defence industry policy. The policy will also assist the Government meet its commitment to strengthening connections between science, research and industry and building new ones[10].

Second, given the breadth and diversity of the national security S&T community and the challenges they must address, the policy must create the environment and mechanisms to facilitate a more coherent whole-of-government coordinated approach to delivering national security S&T. Currently, there is no national, strategic and coordinated approach to planning and funding S&T to support national security in the most efficient manner. The policy must facilitate stronger integration of effort by bringing together Australia's national security agencies (with roles in national security operations and capability development) and Australia's scientific enterprise (with relevant S&T capabilities) to encourage interdisciplinary and cross-sectoral responses to security challenges beyond the capability and capacity of any single agency. The framework will establish new mechanisms, or build on current mechanisms, to leverage existing S&T (including synergies with S&T support for Defence) and increase the proportion of research focused on national security.

Questions for discussion:

Q3.1 Which concepts, principles, actions from NSSIS (2009) (if any) should be incorporated into the new policy and program?

4. The national security S&T policy

4.1 Objectives

The Government's principal intent of a national security S&T policy is to recognise the importance of S&T to the security of Australia and its interests, and to ensure that S&T is appropriately harnessed to continue its valued contribution to our nation's security.

The purpose of the policy will be to:

- define Australia's national security S&T priorities for the next decade;
- coordinate efforts to best take advantage of investment in S&T and address critical gaps to address immediate and future national security capability, operational and policy needs;
- develop and support S&T collaborations and networks that bring together, under a shared vision, the best in industry, academia, PFRAs and government; and
- create public and private investment partnerships in national security S&T through a Program that accords with Government priorities and capitalises on our broader innovation system and international linkages.

[10] Minister for Industry The Hon Ian Macfarlane MP, Science meets Parliament. 18 March 2014.

Questions for discussion:

Q4.1 Are these the right objectives for a national security S&T policy? If not, how should they be articulated?

Q4.2 Are there other objectives that the policy should address?

4.2 Achieving our objectives

Achieving these policy objectives will require strategies or mechanisms that:

- identify the national security capability needs and priorities of user agencies, and the S&T support required to meet those needs,
- coordinates S&T to avoid duplication and leverages existing projects or programs,
- fosters cross-agency interactions and culture to stimulate world class research (e.g. shared state-of-the-art S&T infrastructure),
- facilitates multi-agency co-investment in national security S&T,
- promotes best practice and leverages international partnerships, and
- gives clarity and visibility of Australia's strategic direction for national security S&T.

In endeavouring to meet the Government's desire to reduce red tape and cognisant of the tight financial environment, consideration will be given to leveraging current arrangements (if they exist) or strengthening extant mechanisms where appropriate. This includes accessing, sharing and leveraging related work, skills, knowledge and infrastructure that currently reside in government, universities or industry.

Questions for discussion:

Q4.3 In the spirit of the Government's aim in reducing red tape, are there suggestions or options for achieving national security S&T objectives in a way that it is efficient and minimises bureaucracy?

Q4.4 What current mechanisms exist or what options are there for new ones that facilitate sharing capabilities that reside outside Government?

4.3 Priorities for Australia's national security S&T

A key element of the national security S&T policy will be the articulation of the Government's national security S&T priorities over the 0 to 5 years and then out to 10 years and longer. This serves three important purposes. First, it will ensure our S&T efforts are directed to our most significant national security challenges. Second, it will guide the allocation of resources towards addressing Australia's most pressing national security priorities. Third, it will help give universities, industry and other S&T providers' clarity and some certainty around where they can focus and best serve Australia's national security agencies.

There are a number of complex national security problems facing Australia over the next decade which will warrant significant and sustained S&T support and resourcing from public and private sectors (e.g. harmful cyber activity; proliferation of weapons of mass destruction; ready availability of new technology to malicious actors such as 3D printing, bioengineering and advances in material sciences; terrorism; espionage; serious and organised crime). By setting strategic national security S&T priorities or themes, the national security S&T community can better plan, invest and execute a coordinated national security S&T program of sufficient scale and quality to achieve required national security outcomes.

The following five themes are proposed as priorities for national security S&T areas for Australia. In the main, they are consistent with priorities identified by national security S&T community stakeholders in 2009[11] and in 2011[12], while giving greater emphasis to S&T priorities in Cyber Security and Border Protection and Identity Management. They also recognise existing cross-agency coordination mechanisms that may be utilised to elicit user requirements, and for program delivery and reporting (e.g. intelligence forums, biometrics interdepartmental committees, Operation Sovereign Border etc). They will be refined through consultation and defined in the national security S&T policy. They will provide strategic guidance and scope for the supporting Program.

Cyber Security

Challenge: Australia is now dependent on cyberspace for its national wellbeing and security. Cyberspace is an environment vulnerable to exploitation by malicious actors. Cyber security requires application of S&T to anticipate vulnerabilities, strengthen cyber systems and enhance national capacity to respond to and recover from cyber attack.

S&T Scope: Cyber threat estimation and forecasting (e.g. impact of wireless networks, mobility cloud computing), cyber influence and data analytics, sensing to effects, autonomous systems and system design for uncertainty.

Intelligence Exploitation

Challenge: The deluge of available data from heterogeneous sources is challenging the capabilities of agencies to extract actionable intelligence, requiring the support of automated data analysis and representation tools.

S&T Scope: S&T supporting intelligence collection and analysis within the NIC. An alternative broader engagement would also support intelligence applied to criminal investigations.

Border Security and Identity Management

[11] www.dsto.defence.gov.au/national security
[12] www.dsto.defence.gov.au/national security

Challenge: Preserving Australia's border integrity key challenge for Government. The projected growth in people and cargo movement across Australian borders is challenging Customs' ability to identify and assess risks and to conduct timely interventions.

S&T Scope: Biometrics systems, surveillance and detection technologies (wide area, passenger and cargo screening).

Preparedness, Protection and Incident Response

Challenge: Ensuring Australian agencies are appropriately equipped and prepared to effectively and safely respond to events of national security significance, such as a terrorist attack on critical infrastructure or mass gatherings.

S&T Scope: S&T supporting the first responder community infrastructure protection, national security exercise support and training, social resilience and community engagement.

Investigative Support and Forensics

Challenge: Novel, adapted and complex methods used by terrorists and perpetrators of nationally significant crimes creates an ongoing need for S&T assisted solutions to detection, investigation and prosecution.

S&T Scope: S&T supporting investigation of nationally significant and transnational crime and domestic terrorism (e.g. detection and surveillance technologies, intelligence, collection and analysis, forensic analysis).

Cyber Security – a priority for a whole of nation S&T effort

Cyber security is a national security priority. Australia is dependent on an increasingly vulnerable cyber environment. Cyber is advanced and shaped by technology. The pace of technological development and Australia's accelerating reliance on complex, interconnected systems drives the imperative to fully exploit S&T innovation in combating and containing cyber intrusions, and in hardening protection of critical infrastructure information and communication technology (ICT) vulnerabilities. Nurturing, harnessing and orchestrating resources to focus on this national problem are essential.

For these reasons, the Government intends to initially focus on establishing a national Cyber Security S&T program. The program will support the monitoring, management and protection of Australia's cyber enabled enterprise. It will focus on aiding, enhancing and future-proofing the Australian Cyber Security Centre (ACSC) capability; advanced tools and techniques particularly for ACSC transition of technology and processes to national networks; and establishing national S&T workforce and skills that are relevant and responsive to operational cyber security needs.

Questions for discussion:

Q4.5 Do these priorities address the most significant national security challenges Australia will face over the coming decade, and which warrant a collective, strategic approach to the application of S&T effort?

Q4.6 Is the scope of these priorities appropriate? If not, what would be more appropriate?

Q4.7 Are there other priorities the Government should consider in the immediate future? (0-3 years)

Q4.8 What specific cyber threats and/or mitigations should be considered in developing a cyber S&T program? Who are the key stakeholders that should be involved?

4.4 Improving coordination

The national security S&T community is a diverse stakeholder group (refer to Section 2.2). It comprises public and private sector organisations performing a wide range of functions (e.g. policy development, emergency response, policing, intelligence gathering and analysis, scientific research, technology development) and individuals with a wide range of skills to perform those functions. Unfortunately the paucity of coordination mechanisms lends itself to national security S&T stakeholders operating independently, focusing on their own particular priorities and issues and building their own partnerships with S&T providers to address them. While in some cases this may be entirely appropriate, coordination across stakeholders can address many strategic security challenges. Better coordination can also help to quickly build up the knowledge of how S&T can be further developed and used operationally by user agencies, as well as providing a good way of identifying lessons learned. However, effective coordination is intrinsically difficult. One aspect of this difficulty revolves around accessing and sharing sensitive information.

The policy will provide the framework to enhance coordination by:

1) building and nurturing important trusted partnerships and networks between user agencies and S&T providers,

2) improving awareness of and access to S&T capabilities and expertise, and

3) identifying opportunities to leverage and synergise research programs that are of national security interest.

Key coordination strategies may include (but are not limited to):

- leveraging existing coordinating committee structures (such as ANZCTC, ANZEMC), and
- raising awareness through dissemination across the national security community, of information, data and research outcomes of national security relevance (through conferences,

workshops, websites, portals, databases, scientific adviser networks). This will require standardised and robust arrangements for sharing classified information.

Questions to discuss

Q4.9 Are these coordination approaches appropriate? If not, why not? Are there other coordination challenges?

Q4.10 What extant coordinating committees could be better utilised?

Q4.11 Given the transfer of the coordination function from PM&C to Defence, what might be the issues that Defence needs to pay particular attention to?

4.5 Improving governance

Establishing effective governance arrangements will be critical to achieving the objectives of the national security S&T policy and for developing and delivering an S&T program.

The purpose of the governance arrangements will be to:

- provide strategic oversight of and guidance to the National Security S&T Program,
- give primary stakeholders a role in strategic decisions on the Program,
- ensure effective use of Commonwealth resources by ensuring the right research is being done, by the most appropriate providers,
- ensure the research team/s are held accountable for their deliverables, and
- provide assurance of the quality and impact of the research.

A two tiered governance arrangement is proposed, comprising a Steering Committee and working groups.

The Steering Committee will provide strategic leadership for the National Security S&T Program and will advise on the balance of investment across the national security S&T priorities to ensure alignment and consistency with Government policy.

The Chief Defence Scientist will convene and lead the cross agency Steering Committee with representatives drawn from, but not be limited to:

a. the Department of Defence;
b. the Attorney General's Department;
c. the Department of Prime Minister and Cabinet;
d. Australian Security Intelligence Organisation;
e. the Australian Federal Police;
f. the Australian Customs and Border Protection Service;
g. Commonwealth Scientific and Industrial Research Organisation;
h. Australian Nuclear Science and Technology Organisation;
i. Department of Industry

Other agencies with an interest in national security S&T may be invited to participate in the Steering Committee as required. DSTO will be responsible for the secretariat of the Steering Committee and matters of administration. All representatives of the member agencies should be Senior Executive Service officers.

The Steering Committee will oversee the development of working groups on specific areas within the national security S&T priorities. These working groups will comprise representatives of national security user agencies, PFRAs, academia and industry. These groups will be responsible for collating user requirements (which may include using extant cross agency national security committees such as the ANZCTC) and determining the most appropriate S&T response/s (ie. projects, deliverables etc) to meet those requirements. They will also facilitate information sharing across user agencies and S&T providers.

The national security S&T policy will realise the leadership role of DSTO as Australia's national security S&T coordinator and program manager. As the coordinator, DSTO will be the first point of contact for identifying needs and resolving S&T approaches for the national security community. It is the DSTO's role to facilitate and build the relationships required to meet the policy's objectives and manage mechanisms to deliver outcomes for user agencies. It will implement and administer the governance and coordination arrangements to bring together user requirements, resources, interests and organisations. DSTO will be the repository of this information and a conduit for sharing across the national security S&T community.

Questions for discussion

Q4.12 Do the proposed governance arrangements meet the overall policy objectives? Are there alternatives that would meet the policy objectives in a more efficient and effective way?

Q4.13 Is the composition of the steering committee appropriate? Are there stakeholders that should/should not be represented and why?

Q4.14 Should the steering committee be co-chaired by a user agency? Why or why not? What agency/s could co-chair?

Q4.15 Where should the steering committee report into? e.g. National Security Committee of Cabinet?

Q4.16 What are your expectations of DSTO as Australia's coordinator for national security S&T?

4.6 Promoting collaboration and innovation

Collaborative partnerships between government, industry and academia are important to achieving innovative and efficient national security outcomes and are a key objective of the national security S&T policy and program. A multidisciplinary approach is critical to understand and address national security issues, particularly as problems and solutions become more complex. Collaboration can also contribute to increased productivity, greater transfer of advanced technology and knowledge, access to niche areas of world class research and infrastructure, and acceleration of technology transfer and commercialisation.

Effective collaboration requires an ongoing relationship to learn about the needs of the national security community or the agency in order to earn respect and trust. In the absence of trust, the quality of research and the extent of information sharing across the community may be compromised. To foster effective collaborations the policy will establish mechanisms that:

- recognise, manage and support the interests, needs and constraints of all partners,
- clearly identifies leadership roles, responsibilities and accountabilities, and resolves any issues, and
- balances the scholarly needs of academic researchers with the application of their expertise to achieve tangible outcomes for the national security user agencies.

The policy will promote a greater role for industry in national security S&T, recognising not only their niche R&D capabilities but their role in bridging the 'valley of death' in the research and commercialization pathway. This will also align with the Government's commitment to support Australia's industry sector – from large multinationals through to small to medium enterprises[13].

The challenge in sharing the delivery of S&T with non-government partners is the risk that their participation will only materialise where there are clear commercial benefits or incentives for them to do so. Given that the primary objective of this program is to address national security problems, a clear beneficiary must be the national security user agencies. For some companies particularly those with experience in collaborating with government in the Defence industry sector, will appreciate that these partnerships gives them privileged access to government strategy and planning and access to Australia's best researchers and institutions. It gives them insight and visibility of government priorities to align their business to, and reduce their cost of participating in research.

Goals for improving collaboration include:

- enhance ability of the national security agencies to participate actively in research agenda setting, and
- creating incentives for collaboration (e.g. seed funding to co-investment collaborations, access to information, data, tools and technologies).

Questions for discussion

Q4.17 What other barriers to collaboration exist and how might they be managed?

Q4.18 What models to improve collaboration exist? What works, and what does not?

[13] Liberal Party of Australia (2013). '*Our Plan, Real Solutions for all Australians*.' http://www.liberal.org.au/our-plan

5. A National Security S&T Program

To meet the Government's national security S&T policy objectives a National Security S&T Program will be established to coordinate the planning, management and delivery of S&T projects. The Program will:

- address the Government's national security S&T priorities set out in the national security S&T policy (see Section 4.3),
- be user focused and outcome driven,
- provide S&T support that meets short and long term capability and operational requirements of national security agencies,
- seek efficiencies by identifying and addressing S&T requirements shared across agencies,
- capitalise on S&T expertise and infrastructure residing across the national innovation system and outside the national security context and building capacity where required,
- leverage existing partnerships, nationally and internationally, or build new ones where required and
- align and contribute to broader government policy and programs in science and research, productivity, industry and international development.

Program development will follow a 'top-down bottom-up' process. The 'top down' approach will see the Program get its strategic direction from the Government's national security S&T priorities. The 'bottom up' approach will utilise working groups (see Section 4.6) to then collate the user requirements, plan and oversee the delivery of specific projects to meet those requirements. The scope, scale and duration of these projects will vary depending on the user requirements. Projects will lie along a spectrum from short term research (months-2 year timeframe), to fill immediate operational capability gaps and/or transition prototypes into operational capability, mid-term research (2-3 year timeframe) intended to transition concepts into demonstration of new and enhanced capabilities, to long term research (3-5 year duration) intended to fill knowledge gaps and develop future capability concepts.

5.1 A collaborative co-investment delivery model

The National security S&T Program will be based on a collaborative co-investment model. Resourcing will leverage contributions (cash and in kind) from user agencies, S&T providers and where appropriate, international partners. This leverages S&T capacity to undertake activities that are beyond the scope of any one organisation. It will draw on (or where appropriate integrate into) elements of extant models within Defence such as the Rapid Prototyping, Development and Evaluation Program[14], the Defence Material Technology Centre[15] and the Capability Technology Demonstrator Program[16], and outside the Defence environment, such as the Cooperative Research Centres[17] and ARC Centres of Excellence[18].

[14] http://www.rpde.org.au/
[15] http://dmtc.com.au/

The following are key aspects of the collaborative co-investment model.

- Research will involve national security user agency staff and S&T experts working closely together to deliver innovative user focused outcomes.
- Research will be undertaken by S&T providers with a diversity of skills and expertise from across universities, PFRAs and/or industry (nationally and internationally).
- Research projects can be short, medium and long-term (1-5 years) and must address specific user requirements and deliver specific outputs and outcomes agreed by user agencies.
- Projects will be funded through multiple sources from each of the research participants – government and non-government, cash or in-kind.
- Progress is monitored, with flexibility to modify the project if the needs of users change or if the science shows a more viable alternative or, to cease the science promises inadequate value.

5.2 Process

The development, management and monitoring and reporting of the National Security S&T Program will take place on an annual cycle, encompassing the following steps.

Defining the problem

For each national security S&T priority area, a working group (comprising representatives from user agencies, PFRAs, universities and industry) will identify and prioritise user requirements, define specific S&T projects and deliverables to address those requirements and their estimated cost.

Coordinating the Program

DSTO will coordinate information from across all priorities, identify any overlap and synergies with other user requirements or currently funded research programs, and make refinements as required.

Endorsement of the Program

The Program and the allocation of government resources across the Program will be endorsed by the Steering Committee.

Sourcing S&T support and reporting

DSTO will initiate a request for project proposals to address the S&T projects. These projects may be for either short, medium to long term duration. Proposals should be fully costed and applicants would be expected to self-organise their collaborative partners and co-investment arrangements. Proposals could be either short-listed to submit full proposals, or may be assessed in one process. The Steering Committee and/or the relevant user agency/s would be consulted in the decision process. DSTO would administer, manage and review the project proposals and project reports.

---

[16] http://www.dsto.defence.gov.au/ctd/
[17] https://www.crc.gov.au/
[18] http://www.arc.gov.au/ncgp/ce/

Questions for discussion

Q5.1 What other collaborative, co-investment models warrant consideration? What has worked, what hasn't worked?

Q5.2 What are the pros and cons of a collaborative co-investment delivery model for national security S&T.

Q5.3 Which would be your preferred option for a collaborative co-invested model? Are there others?

6. Implementation

Implementation will take a staged approach, focusing initially on establishing appropriate coordination and governance arrangements and developing a Program that meets the national security problems of highest priority to government, such as Cyber Security. The level of effort and resources will match the staged approach with more critical and high priority activities being given greater attention and resources in the first 5 years. The details of the implementation plan and costings will be developed in consultation with stakeholders and agreement sought from Government.

6.1 Implementation priorities

In the first stages of implementation, priority will be given to:

- establishing new governance arrangements including a National Security S&T Steering Committee and its Terms of Reference,
- establishing a collaborative co-funded model and processes for developing and delivering the National Security S&T Program,
- developing mechanisms to facilitate collaborative multi-organisational partnerships,
- a communication strategy to engage stakeholders in implementation, including continuation of workshops,
- examination of existing international national security S&T collaborations, to re-examine focus on national and shared priorities with the US Department of Homeland Security and the US Combating Terrorism Technical Support Office, and expand collaboration to include the UK Home Office, and
- defining and initiating a number of S&T projects under approved priority areas (initially Cyber Security) and priority 'seed' projects in other priority areas.

6.2 Monitoring, review and evaluation

The Steering Committee will be responsible for monitoring, reviewing and evaluating the implementation of the National Security S&T policy and Program to ensure transparency and accountability. An annual reporting process will be instituted and findings communicated widely. Stakeholders will be able to see how implementation is tracking against key milestones and will be

involved in decisions about any changes that may be required through their representation on the Steering Committee and/or working groups.

Evaluation and review to demonstrate success of the policy and program will be of limited value without establishing a baseline. Baseline data will be established as part of the early implementation phase so that monitoring data is comparable and collected consistently.

Questions to discuss

Q6.1 What specific barriers or challenges may impact the effectiveness of monitoring, review and evaluation? How might these be overcome?

Q6.2 What baseline data should be collected and how?

6.3 Resource management

Implementation will be staged and resource allocations will shift accordingly. Overall, it is anticipated that resources will be required for the following functions:

- administration and coordination of the National Security S&T Program,
- S&T delivery, and
- governance and reporting.

The governance arrangements will provide transparency over resource allocation across the Program and help overcome challenges to collaboration where there are cross agency and/or government and non-government funding sources and where complex accountability mechanisms exist.

Questions to discuss

Q.6.3 Are there any other resource management issues to be considered?

Glossary of abbreviations

ACC	Australian Crime Commission
ACPBS	Australian Customs and Border Protection Service
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
ANZCTC	Australia-New Zealand Counter-Terrorism Committee
ANZEMC	Australia-New Zealand Emergency Management Committee
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AusAID	Australian Agency for International Development (ceased operation and integrated into the Department of Foreign Affairs and Trade on 31 October 2013)
DAFF	Department of Agriculture, Fisheries and Forestry (since renamed Department of Agriculture)
Defence	Department of Defence
DFAT	Department of Foreign Affairs and Trade
DoHA	Department of Health and Ageing (since renamed the Department of Health)
DIAC	Department of Immigration and Citizenship (since renamed Department of Immigration and Border Protection)
DIT	Department of Infrastructure and Transport (since renamed Department of Infrastructure and Regional Development)
NIC	National Intelligence Community (or Australian Intelligence Community) is an informal term describing the six Australian security and intelligence agencies – the Office of National Assessments (ONA); the Australian Security Intelligence Organisation (ASIO); the Australian Secret Intelligence Service (ASIS); the Australian Signals Directorate (ASD); the Defence Intelligence Organisation (DIO) and the Australian Geospatial-Intelligence Organisation (AGO).
ONA	Office of National Assessments
PM&C	Department of the Prime Minister and Cabinet